

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

Geoff Dittberner and Mary Wint,  
individually and on behalf of themselves  
and all others similarly situated,

Plaintiffs,

V.

University of Minnesota,

Defendant.

Case No.

# CLASS ACTION COMPLAINT

## Jury Trial Demanded

Plaintiffs Geoff Dittberner and Mary Wint (collectively, “Plaintiffs”), by their undersigned counsel, file this Class Action Complaint on behalf of themselves and a class of all similarly situated persons against Defendant University of Minnesota (“UMN” or “Defendant”). Plaintiffs base the forgoing allegations upon personal information and belief, the investigation of counsel, and state the following:

# INTRODUCTION

1. UMN is a public research university with multiple campuses throughout the State of Minnesota. UMN is the oldest and largest in the University of Minnesota system and has the ninth-largest main campus student body in the United States, with more than 50,000 students annually. UMN claims to have “50,000+” students and “485,000” living

alumni.<sup>1</sup> UMN claims to be “[a]n [i]ndispensable [e]ngine for Minnesota” that “contributes more than \$8.6 billion a year in economic activity to the state.”<sup>2</sup>

2. Students, employees, applicants, and others affiliated with the UMN provide it with highly sensitive personal information, including Personally Identifying Information (“PII”) including, among other things, names, addresses, telephone numbers, email addresses, and social security numbers. UMN gathers this information and stores it on its servers in a database.

3. This type of personal and sensitive data is highly targeted by hackers who seek to exploit this data for nefarious purposes. Indeed, PII and, in particular, social security numbers, have inherent value, and are routinely marketed and sold on the dark web. In the wrong hands, the personal and sensitive data that UMN collects and stores may be utilized to cause significant harm to the those who provided this information, including being used to orchestrate a swath of fraudulent schemes.

4. The value of this information on the dark web is well recognized in the modern data economy, and the foreseeable risk to customers’ identities as a result of a criminal hacking event is known and recognized by technology companies that gather and store data, including Defendant.

5. UMN gathers, stores, and uses sensitive information it gathers from students, applicants, employees, and other individuals, including social security numbers. As such, UMN has a duty to protect the sensitive data it chooses to store. UMN recognizes the

---

<sup>1</sup> *About Us*, UMN (last visited, Aug. 22, 2023), <https://twin-cities.umn.edu/about-us>

<sup>2</sup> *Id.*

importance of protecting this data. Indeed, it admits to being governed by the Minnesota Government Data Practices Act and cannot release personally identifying information without consent.<sup>3</sup> Further, under Minn. Stat. § 13.05, subd. 5(2) of the Minnesota Government Data Practices Act, entities like UMN must “establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only accessed by those persons for purposes described in the procedure.”

6. Despite these requirements and its understanding of the need to implement reasonable security measures to keep students and employees’ information safe, UMN failed to do so. Instead, a hacker active on the dark web with a username of “niggy” reported that he infiltrated UMN’s database and gained access to PII and other sensitive information, including over 7 million unique social security numbers (“Data Breach”). The stolen information includes data from digitized records initially created as far back as 1989.

7. It appears UMN did not learn that the hacker had infiltrated its systems, gained control over them, and stole millions of social security numbers until after the hacker had successfully infiltrated its system and exfiltrated millions of individuals’ data. Indeed, UMN only just started investigating the Data Breach as of July 21, 2023. The hacker has already purported to have made the information available on the dark web.

---

<sup>3</sup> <https://privacy.umn.edu/>

8. The Data Breach has already had serious consequences and will continue to do so. As a direct and proximate result of UMN's inadequate data security and the resulting data breach, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including: (i) from the untimely and inadequate notification of the Data Breach, (ii) the diminished value of their personal information; (iii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iv) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (v) out-of-pocket expenses for securing identity theft protection and other similar necessary services; and (iv) emotional harm and distress from the exposure of their sensitive records and the prolonged and heightened risk of harm.

9. Plaintiffs, therefore, bring this Class Action Complaint seeking relief for their injuries and those of persons who were similarly impacted by the Data Breach and inadequate data security.

### **JURISDICTION**

10. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Here, minimal diversity is met under CAFA because at least one member of the proposed Class is diverse from the Defendant. UMN is located

and operates exclusively in the State of Minnesota and is a citizen of only that State. The Class is comprised of applicants to attend UMN, and current and former students and employees of UMN, which includes individuals dispersed throughout the country and who are citizens of States other than Minnesota. Plaintiffs allege that, in the aggregate, the claims of all putative class members exceed \$5,000,000, exclusive of interest and costs.

11. This Court has general personal jurisdiction over UMN because UMN is located entirely within the State of Minnesota, and is a Minnesota public institution operating on behalf of the State of Minnesota. UMN has minimum contacts with Minnesota because it is located there and conducts substantial business there, and Plaintiffs' claims arise from UMN's conduct in Minnesota, including because UMN's database containing the information stolen is located in Minnesota.

12. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in Minnesota and because UMN conducts a substantial part of its business within this District.

### **PARTIES**

13. **Plaintiff** Geoff Dittberner is a citizen of Minnesota residing in Inver Grove Heights, Minnesota. Dittberner applied to attend school as an undergraduate at the UMN in 2012. In his application, he provided UMN with his PII, including his name, contact information, social security number, and date of birth, among other information. He was accepted to the UMN and attended from 2012 to 2015, and returned to UMN in 2019 to complete his undergraduate degree. Additionally, from 2012 to 2013, Dittberner worked

as a Government Relations Office Assistant at UMN. As an employee, he again provided UMN with his PII, including his social security number and date of birth, among other information. Dittberner, as an applicant and student at and employee of the UMN, reasonably believes his PII was stolen from UMN, especially because the stolen information includes a folder containing applicant data dating back to 1989.

14. **Plaintiff** Mary Wint is a citizen of Minnesota who resides in Mora, Minnesota. Wint worked at the UMN as an employee for approximately 20 years. Specifically, she worked at the UMN as a Nutrition Educator for Kanabec and Millie Lacs counties from 1993 to 2013. She is also a patient of the UMN's health care system. As part of her employment and as a patient at UMN, she provided her PII, including her name, contact information, social security number, and date of birth, among other information. Wint, as a long-term employee of and patient at the UMN, reasonably believes her PII was stolen from the UMN because the Data Breach purportedly impacted students and staff.

15. **Defendant** University of Minnesota, or UMN, is a higher education public institution in the State of Minnesota that accepts applicants to its undergraduate and graduate programs from people throughout the United States and from non-U.S. born individuals. It, furthermore, employs thousands of staffs in academic and non-academic roles.

## BACKGROUND

### A. UMN Collects Personal and Sensitive Information from Students, Employees, Applicants and Others

16. UMN is one of the nation's premier public higher education institutions. Annually, it accepts thousands of applicants into its undergraduate and graduate programs. It, furthermore, employs thousands of employees to maintain its operations. As of 2022, UMN employed 4,033 academic staff, over 24,000 staff in general, and had nearly 55,000 students, including 30,560 undergraduates, 11,613 postgraduates, and 3,875 doctoral students.

17. From its applicants, students, employees, and potential others, UMN collects highly sensitive PII, including names, addresses, telephone numbers, email addresses, birth dates, and social security numbers. Indeed, as part of its application process, UMN's online application portal requires U.S.-born applicants to provide their social security numbers:

The screenshot displays the 'Personal Information' section of the University of Minnesota Golden Gopher Application portal. The browser address bar shows 'umntc.mycollegeapplication.org/profile/PersonalInfo.aspx'. The page header includes the University of Minnesota logo and 'Driven to Discover™'. The navigation bar features 'Home', 'About You' (highlighted), 'Education', 'Activities', 'Short Answers', and 'Review / Submit'. The 'About You' sidebar lists 'PERSONAL INFORMATION' (highlighted), 'ADDRESS', 'ETHNICITY & RACE', 'RESIDENCY', and 'FAMILY BACKGROUND'. The main form area is titled 'Personal Information' and includes instructions: 'Fields marked with "\*" are required.' and 'Please enter your legal name as it is indicated on your official government identification, such as passport or driver's license.' The form contains input fields for 'First Name \*' (filled with 'Goldy'), 'Middle Name' (placeholder 'Enter your Middle Name'), and 'Last Name \*' (filled with 'The Gopher'). Below these are checkboxes for 'I'd like to use a different name when communicating with the University of Minnesota Twin Cities.' and 'My name is different on previous records.' The 'Date of Birth \*' field is filled with '5/11/1958' and includes a calendar icon. The 'Social Security Number' field is highlighted in yellow and is currently empty.

18. Each year, UMN receives tens of thousands of applicants and employs tens of thousands of academic and non-academic staff. Consequently, the UMN has built up a massive repository of sensitive information on millions of individuals.

19. UMN understands the importance of securing the highly sensitive PII that it collects and stores in its database. UMN, as a public institution, is governed by the Minnesota Government Data Practices Act (“GDPA”), Minn. Stat. § 13, *et seq.* The GDPA governs “all governmental entities” and was enacted to regulate the “collection, creation, storage, maintenance, dissemination, and access to government data in government entities.” Under the GDPA, government entities have obligations with respect to the data it collects and stores, including: (1) establish[ing] appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure”; and “developing a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.” *Id.* at § 13.05, subd. 5(a)(1)–(2).

20. The GDPA, similarly, requires that “[w]hen not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.” *Id.* at subd. 5(b). The GDPA also required, starting more than two decades ago, that governmental entities “appoint or designate . . . [a] data practices compliance official” to resolve “problems in obtaining access to data or other data practices problems.” *Id.* at subd.

13.

21. Furthermore, the GDPR required UMN to obtain annual security assessments of any personal information maintained by the government entity. *Id.* at § 13.055, Subd. 6. Highlighting the significance of protecting data against unauthorized disclosure, when a breach does occur, the GDPR requires government entities to notify impacted individuals “in the most expedient time possible and without unreasonable delay . . . .” *Id.* at Subd. 2(a).

22. UMN acknowledges its obligations to protect data under the GDPR, indicating that it is well aware of the importance of security data against unauthorized access.<sup>4</sup>

23. Despite its knowledge, UMN failed to enact measures sufficient to protect against a data breach. In August 2023, a hacker known as “niggy” released millions of social security numbers and other PII stolen from a UMN database.

**B. UMN’s Inadequate Data Security Measures Exposed Plaintiffs’ and the Class’s PII**

24. On August 22, 2023, the University of Minnesota confirmed that it had contacted law enforcement concerning a potential data breach that it became aware of on July 21, 2023.<sup>5</sup> Specifically, representatives of the UMN stated that they became aware that an “unauthorized party” had claimed to possess sensitive data taken from the UMN’s computer systems.<sup>6</sup>

---

<sup>4</sup> <https://privacy.umn.edu/>

<sup>5</sup> <https://www.kare11.com/article/news/local/u-of-m-investigating-claimed-data-breach/89-17a1736f-a704-4495-9337-079e0c77ccd5>

<sup>6</sup> *Id.*

25. The UMN became aware of the data breach from disclosures made by the purported hacker. On July 21, 2023, a hacker with a username “niggy” posted on the dark web and claimed to have accessed UMN’s database and obtained sensitive information, including social security numbers, for over 7 million unique individuals.<sup>7</sup> The hacker exploited a Computer Network Exploitation or “CNE”, which is often used to infiltrate a target’s computer networks to extract and gather data. The hacker here successfully breached UMN’s database, uncovering sensitive information dating back to records initially created in 1989 and later digitized.<sup>8</sup>

26. The leaked information on the dark web reportedly listed in two tables, one named “PS DIVERSITY”, concerning diversity statistics, and another named “PS\_DWAD\_APPL\_DATA\_HS”, which involves admission statistics.<sup>9</sup> Although the scope of the data breach is not clear, the data of those applying to be admitted to UMN is included in the PS\_DWAD\_APPL\_DATA\_HS table, indicating tens if not hundreds of thousands of individuals have had their data stolen and posted o the dark web.

27. Moreover, former UMN regent Michael Hsu warned that “Everyone should be concerned” because “even if you are a former student or staff you still have data in the university system[.]”<sup>10</sup>

---

<sup>7</sup> <https://thecyberexpress.com/university-of-minnesota-data-breach/>

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> <https://www.kare11.com/article/news/local/u-of-m-investigating-claimed-data-breach/89-17a1736f-a704-4495-9337-079e0c77ccd5>

28. Mark Lanterman, the chief Technology Officer at Computer Forensic Services, warned that anyone potentially affected by the Data Breach should freeze their credit reports to prevent new credit being opened in their name.<sup>11</sup>

29. According to the UMN, they have run scans that have indicated that no additional suspicious activity is ongoing.<sup>12</sup> Thus, the hacker successfully entered into the UMN's networks, gained access to the UMN's database, exfiltrated a significant sum of data, including PII and social security numbers, all without detection by the UMN or any of its security tools or personnel. Indeed, the UMN only became aware of the attack after the hacker publicly described it and posted the stolen data.

30. UMN has known of the Data Breach since at least July 21, 2022.

**C. UMN's Data Breach Caused Plaintiffs' and the Class's Injuries**

31. UMN's Data Breach resulted in the theft and exposure of confidential data, including social security numbers and other PII. Exposure of this type of data puts individuals at a significant and prolonged risk of fraud and identity theft. Indeed, personal information like that stolen from UMN is valuable and has been commoditized in recent years because of its use in conducting identity theft and fraud.

32. After a data breach like UMN's, the hackers responsible for the breach increasingly seek to sell the stolen personal and sensitive records on the black market to

---

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* 5

purchasers looking to use the personally identifying information to create fake IDs, make fraudulent transactions, obtain loans or commit other acts of identity theft.<sup>13</sup>

33. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. Personal and sensitive data, like the type exposed in UMN's Data Breach, is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers and including data not found in other breaches. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud, and can use stolen usernames and passwords to steal additional personal and sensitive information from other applications and websites.<sup>14</sup>

34. Consequently, stolen personal and sensitive data is often trafficked and sold on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

35. Stolen sensitive data sold on the dark web has proven to be valuable. For instance, cybercriminals on the dark web have sold Social Security numbers for up to \$300 per number to be used on fraudulent tax returns. UMN's data breach exposed social security numbers, which are already available on the dark web.

---

<sup>13</sup> *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), <https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/>

<sup>14</sup> FTC Consumer Information, *What to Know about Identity Theft*, [ftc.gov](https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft) (last visited, Aug. 13, 2021), <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>

36. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by reiterating that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”<sup>15</sup>

37. Given the value of that data, a robust cyber black market exists in which criminals openly post and purchase stolen personal information on the dark web.

38. As such, the ramifications of Defendant’s failure to keep Plaintiffs’ and the Class’s personal information secure are severe.

39. When sensitive personal data is stolen, the risk of identity theft is lasting. The U.S. Government Accountability Office’s research into the effects of data breaches found that “in some cases, stolen data may be held for up to a year or more before being used to commit identity theft.

40. Once stolen data has been sold or posted on the web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot rule out the significant risk of future harm.”<sup>16</sup> Indeed,

---

<sup>15</sup> Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Sept. 22, 2021), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

<sup>16</sup> Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (Jun. 2007), <http://www.gao.gov/new.items/d07737.pdf> (last accessed Nov. 30, 2018).

according to experts, one out of four data breach notification recipients are later victimized by identity fraud.<sup>17</sup>

41. Additionally, after personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can allow hackers to harvest additional sensitive and confidential information from the victim, as well as the personal information of family, friends, and colleagues of the initial victim.

42. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant here did not rapidly report to Plaintiffs and the Class that their personal information had been stolen and, in fact, have not yet reported the full extent of the Data Breach.

43. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Using data stolen in data breaches like UMN's, hackers and other wrongdoers may use consumers' personal and

---

<sup>17</sup> *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (last visited Sept. 22, 2021), <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/>

financial information to siphon money from existing accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

44. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

45. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their personal information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

46. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen personal information. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

47. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.<sup>18</sup> According to the FTC, data security

---

<sup>18</sup> *Start With Security, A Guide for Business*, FTC (last visited Sept. 22, 2021), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry unapproved activity; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.<sup>19</sup>

48. According to the FTC, unauthorized personal information disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.<sup>20</sup> The FTC, as such, treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

49. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Defendant] allowed users to bypass authentication procedures” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) (“[Defendant] failed to employ sufficient measures to detect unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008)

---

<sup>19</sup> *Id.*

<sup>20</sup> Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012) (last visited Sept. 22, 2021), [www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf](http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf).

(“[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s Inc.*, No. C-4291 (May 20, 2010) (“[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization” and “failed to use readily available security measures to limit access between instore networks . . .”). These orders, which all preceded UMN’s Data Breach, further clarify the measures businesses must take to meet their data security obligations.

50. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their personal information. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that “[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US \$30.49–44.62.”<sup>21</sup>

51. By virtue of the Data Breach here and unauthorized release and disclosure of the personal information of Plaintiffs and the Class, UMN deprived Plaintiffs and the Class of the substantial value of their personal information, to which they are entitled. As

---

<sup>21</sup> Il-Horn Hann et al., *The Value of Online Information Privacy* (Oct. 2002) available at <http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited Sept. 22, 2021); see also Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

previously alleged, UMN failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

52. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

53. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

54. Even absent any adverse use, consumers suffer injury from the simple fact that their PII has been stolen. When personal information, especially social security numbers, is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. In short, this information can no longer guarantee Plaintiffs and the Class's identities.

55. As a direct and proximate result of UMN's wrongful actions and omissions here, Plaintiffs and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including: (i) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iii) out-of-pocket expenses for securing identity theft protection and other similar necessary services; (iv) the diminution in value of their social security numbers and other private information, the value of which is derived from its confidentiality and privacy; and

(v) emotional distress caused by the impending risk of fraud and identity theft and the loss of privacy, confidentiality, and value of their personal information.

### CLASS ALLEGATIONS

56. Plaintiffs brings this action on behalf of themselves and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

All individuals whose PII was stolen from UMN during its Data Breach

57. Excluded from the class is UMN and its subsidiaries and affiliates; all employees of UMN; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

58. Plaintiffs reserve the right to, after conducting discovery, modify, expand or amend the above Class and Subclass definitions or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

59. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiffs believe that there are millions of members of the Nationwide Class. The number of reportedly impacted individuals already exceeds 7 million U.S. individuals—and each persons' information is readily available to download on the dark web. The precise number of class members, however, is not yet known to Plaintiffs. Class

members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

60. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

- a. Whether UMN knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;
- b. Whether UMN controlled and took responsibility for protecting Plaintiffs' and the Class's data when it solicited that data, collected it, and stored it on its servers;
- c. Whether UMN's security measures were reasonable in light of the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;
- d. Whether UMN breached the GDPR by implementing and using unreasonable data security measures;
- e. Whether UMN owed Plaintiffs and the Class a duty to implement reasonable security measures;
- f. Whether UMN's failure to adequately secure Plaintiffs' and the Class's data constitutes a breach of its duty to institute reasonable security measures;
- g. Whether UMN's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiffs' and the Class's data;
- h. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

- i. Whether Plaintiffs and the Class were injured and suffered damages or other losses because of UMN's failure to reasonably protect its data systems; and
- j. Whether Plaintiffs and the Class are entitled to relief.

61. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs are typical members of the Class. Plaintiffs and the Class are each persons who provided data to UMN, whose data resided on UMN's servers, and whose personally identifying information was exposed in the Data Breach. Plaintiffs' injuries are similar to other class members and Plaintiffs seek relief consistent with the relief due to the Class.

62. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against UMN to obtain relief for themselves and for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs also have retained counsel competent and experienced in complex class action litigation of this type, having previously litigated numerous data breach cases on behalf of consumers and financial institutions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

63. **Superiority.** Consistent with Fed. R. Civ. P. 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

64. **Injunctive and Declaratory Relief.** Consistent with Fed. R. Civ. P. 23(b)(2), UMN, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

## LEGAL CLAIMS

### COUNT I

#### Negligence

#### (On behalf of the Nationwide Class)

65. Plaintiffs repeat and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

66. UMN owed a duty to Plaintiffs and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiffs and the Class, managed and stored. This duty arises from multiple sources.

67. UMN owed a common law duty to Plaintiffs and the Class to implement reasonable data security measures because it was foreseeable that hackers would target UMN's databases because it contained millions of individuals' valuable PII and, UMN further knew that, should a breach occur, Plaintiffs and the Class would be harmed. UMN alone controlled its technology, infrastructure, digital platforms, and cybersecurity that were exposed during the Data Breach and allowed hackers to breach and steal information

from its database. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiffs and the Class. UMN knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen, and that individual need would continue long after the Data Breach ended. Therefore, the Data Breach, and the harm it caused Plaintiffs and the Class, was the foreseeable consequence of UMN's unsecured, unreasonable data security measures.

68. UMN, furthermore, assumed a duty to protect individuals' data by soliciting sensitive PII, collecting that data, and storing that data in its own databases. In fact, Plaintiffs and the Class were required to social security numbers and other PII in order to obtain employment or apply to attend UMN. UMN was the only entity capable of implementing reasonable measures to protect Plaintiffs' and the Class's sensitive data.

69. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required UMN to take reasonable measures to protect Plaintiffs' and the Class's sensitive data and is a further source of UMN's duty to Plaintiffs and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by entities like UMN of failing to implement and use reasonable measures to protect sensitive data. UMN, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the

basis of UMN's duty to adequately protect sensitive information. By failing to implement and use reasonable data security measures, UMN acted in violation of § 5 of the FTCA.

70. UMN is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring UMN to exercise reasonable care with respect to Plaintiffs and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, UMN was the only entity capable of adequately protecting the data that it alone solicited, collected, and stored.

71. UMN breached its duty to Plaintiffs and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. UMN recognized the need to keep PII confidential and safe from cybercriminals who targeted it. Despite that, UMN implemented unreasonable data security that allowed a single hacker to breach its systems, gain control over them, access its database, and exfiltrate data on millions of individuals, all undetected.

72. UMN was fully capable of preventing the Data Breach. UMN is a sophisticated entity that accounts for one of the most respected public higher education entity in the world. It knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented and used, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. UMN thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

73. As a direct and proximate result of UMN's negligence, Plaintiffs and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes. Plaintiffs, therefore, seek all remedies available under the law for UMN's negligence.

**COUNT II**  
**Negligence *Per Se***  
**(On behalf of the Nationwide Class)**

74. Plaintiffs repeat and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

75. UMN's unreasonable data security measures and failure to timely notify Plaintiffs and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which UMN failed to do.

76. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities like UMN of failing to implement and use reasonable measures to protect individuals' sensitive data. The FTC publications and orders described above also form the basis of UMN's duty.

77. Additionally, the GDPR requires entities like UMN to "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for

purposes described in the procedure[.]” Minn. Stat. § 13.05, subd. 5(a)(1). Additionally, the GDPR requires entities to notify those impacted by a data “in the most expedient time possible and without unreasonable delay . . . .” *Id.* at Subd. 2(a).

78. UMN violated Section 5 of the FTC Act and the GDPR by failing to use reasonable measures to protect Plaintiffs’ and the Class’s PII and sensitive data and by not complying with applicable industry standards. UMN’s conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its databases and the foreseeable consequences of a Data Breach should UMN fail to secure its systems.

79. UMN’s violation of Section 5 of the FTC Act and the GDPR each separately constitute negligence per se.

80. Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) and the GDPR were intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the GDPR were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiffs and the Class.

81. As a direct and proximate result of UMN’s negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury. Plaintiffs, therefore, seek all remedies available under the law for UMN’s negligence *per se*.

**COUNT III**  
**Violation of Government Data Practices Act, Minn. Stat. § 13, *et seq.***  
**(On behalf of the Nationwide Class)**

82. Plaintiffs repeat and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

83. Under the GDPA, a government entity that “violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damages as a result of the violation, and the person damaged . . . may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorneys fees.” Minn. Stat. § 13.08, subd. 1. Furthermore, “[t]he state is deemed to have waived any immunity to a cause of action brought under this chapter.” *Id.* Additionally, the GDPA states that “[a] responsible authority or government entity which violates or purposes to violate this chapter may be enjoined by the district court.” *Id.* at subd. 2.

84. The GDPA governs the UMN and applies to its storage of Plaintiffs’ and the Class’s personal information. Minn. Stat. § 13.01, subd. 1 (“All governmental entities shall be governed by this chapter.”).

85. Under the GDPA, the UMN was required to “establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure.” Minn. Stat. § 13.05, subd. 5(a)(2).

86. Furthermore, the GDPR required UMN to obtain annual security assessments of any personal information maintained by the government entity. *Id.* at § 13.055, Subd. 6. Highlighting the significance of protecting data against unauthorized disclosure, when a breach does occur, the GDPR requires government entities to notify impacted individuals “in the most expedient time possible and without unreasonable delay . . . .” *Id.* at Subd. 2(a).

87. UMN acknowledges its obligations to protect data under the GDPR, indicating that it is well aware of the importance of security data against unauthorized access.<sup>22</sup>

88. However, UMN failed to adopt “appropriate security safeguards” to protect Plaintiffs’ and the Class’s highly sensitive information that it stored in its database. The lack of appropriate security safeguards is made clear by the means by which the Data Breach occurred. Specifically, a single hacker with no apparent history of orchestrating data breaches as part of a cybercrime organization singlehandedly infiltrated UMN, obtained control over its networks and access to its databases, successfully exfiltrated a massive amount of data involving over 7 million individuals, and exfiltrated that data all without detection. UMN had no idea it had been breached and the data on its databases stolen until the hacker publicly disclosed the breach and, by the time UMN began investigating it, the hacker, having succeeded in obtaining a swath of valuable data, had already ceased activity within UMN’s networks and servers.

---

<sup>22</sup> <https://privacy.umn.edu/>

89. UMN, therefore, violated the GDPR.

90. Plaintiffs, furthermore, suffered damage as a result of the Data Breach, which occurred directly because of UMN's violation of the GDPR and its failure to adopt appropriate security safeguards.

91. Specifically, Plaintiffs' and the Class's highly sensitive information has been placed on the dark web where cybercriminals have access to it and opportunity to misuse it. Consequently, the confidentiality, integrity, and value of this sensitive information has been diminished because it can no longer guarantee Plaintiffs' and the Class's identities. Plaintiffs and the Class were also damaged due to the need to expend time, effort, and money monitoring their financial accounts, social media applications and their credit scores to identify any misuse of their data. Plaintiffs, in fact, remained at a heightened and substantial risk of harm due to the misuse of their data which has been placed directly in the hands of criminals. Finally, Plaintiffs suffered emotional distress stemming from the disclosure of their sensitive data and the heightened and prolonged risk of harm they now suffer.

92. Plaintiffs, therefore, seek to recover the damages they suffered and costs and attorneys' fees.

### **PRAYER FOR RELIEF**

93. Wherefore, Plaintiffs, on behalf of themselves and the Class, request that this Court award relief as follows:

- a. An order certifying the class and designating Plaintiffs as the Class Representatives and their counsel as Class Counsel;

- b. An award to Plaintiffs and the proposed Class members of damages with pre-judgment and post-judgment interest;
- c. A declaratory judgment in favor of Plaintiffs and the Class;
- d. Injunctive relief to Plaintiffs and the Class;
- e. An award of attorneys' fees and costs pursuant to the GPDA and as otherwise allowed by law; and
- f. An award such other and further relief as the Court may deem necessary or appropriate.

**JURY TRIAL DEMANDED**

94. Plaintiffs hereby demand a jury trial for all the claims so triable.

Respectfully submitted,

Dated: August 25, 2023

/s/ Brian C. Gudmundson

Brian C. Gudmundson, MN Bar No. 336695

Michael J. Laird, MN Bar No. 398436

Rachel K. Tack, MN Bar No. 399529

**ZIMMERMAN REED LLP**

1100 IDS Center

80 South 8th Street

Minneapolis, MN 55402

Telephone: (612) 341-0400

brian.gudmundson@zimmreed.com

michael.laird@zimmreed.com

rachel.tack@zimmreed.com

Gary F. Lynch

Jamisen A. Etzel

Nicholas A. Colella

**LYNCH CARPENTER LLP**

1133 Penn Avenue, 5th Floor

Pittsburgh, PA 15222

Telephone: (412) 322-9243

gary@lc LLP.com

jamisen@lcllp.com  
nickc@lcllp.com

Christopher D. Jennings  
**JOHNSON FIRM**  
610 President Clinton Avenue  
Suite 300  
Little Rock, AR 72201  
Telephone: (501) 372-1300  
chris@yourattorney.com